Patent Application
Docket No.: A-9158

METHODS AND APPARATUS FOR PROVIDING A PARTIAL DUAL-ENCRYPTED STREAM IN A CONDITIONAL ACCESS OVERLAY SYSTEM

INVENTORS: Howard G. Pinder
William D. Woodward, Jr.
Jonathan Bradford Evans
Anthony J. Wasilewski

CROSS REFERENCE TO RELATED APPLICATIONS

The present application is a continuation-in-part of co-pending application serial no. 10/602,986 entitled "Method for Partially Encrypting Program Data" filed 6/25/03, which was filed simultaneously with applications serial no. 10/602,988 and attorney docket no. A-8919, which were a continuation of App. No. 09/930,901 filed 8/16/2001, which is a continuation of App. No. 09/487,076, filed 1/19/2000, now U.S. Pat. No. 6,292,568, which is a continuation of App. No. 09/126,783, filed 7/31/1998, presently abandoned, which claims the benefit of U.S. Prov. App. No. 60/054,575, filed 8/1/1997; and is a CIP of App. No. 09/111,958, filed 7/8/1998, now abandoned, which claims the benefit of U.S. Prov. App. No. 60/054,578, filed 8/1/1997; and is CIP of App. No. 08/767,535, filed 12/16/1996, now U. S. Pat. No. 6,005,938; and is a CIP of App. No. 08/580,759 filed 12/29/1995, now U.S. Pat. No. 5,870,474, which claims the benefit of U.S. Prov. App. No. 60/007,962, filed 12/4/1995; and is CIP of App. No. 08/415,617, filed 4/3/1995, now U.S. Pat. No. 5,742,677.

The present application descends from an application, which was one of seven original applications with identical Detailed Descriptions. All of these applications have the same filing date and the same assignee. The serial numbers and filing dates of the six applications follow:

Ser. No. 09/127,352, filed 7/31/98, presently abandoned, for which a continuation Ser. No. 09/488,230 was filed on 1/20/2000, which issued as U.S. Pat. No. 6,252,964, and continuation Ser. No. 09/811,085 was filed on 3/16/2001, which issued as U.S. Pat. No. 6,516,412, and continuation Ser. No. 10/287,913 was filed on 11/5/2002, currently pending;

Ser. No. 09/126,921, filed 7/31/1998, which issued as U.S. Pat. No. 6,157,719, for which a continuation Ser. No. 09/135,615 was filed on 8/18/1998, which issued as U.S. Pat. No. 6,424,714;

Ser. No. 09/127,273, filed 7/31/1998, presently abandoned, for which a continuation Ser. No. 09/493,409 was filed on 1/28/2000, which issued as U.S. Pat. No. 6,560,340, and for which continuation 10/377,416 was filed on 3/3/2003, which is currently pending;

Ser. No. 09/127,152, filed 7/31/1998, presently abandoned, for which a continuation Ser. No. 09/488,104 was filed on Jan. 20, 2000, which issued as U.S. Pat. No. 6,246,767; for which continuation Ser. No. 09/748,313 was filed on 12/26/2000, which issued as U.S. Pat. No. 6,526,508; and for which continuation Ser. No. 09/881,428 was filed on 6/14/2001, currently pending;

Ser. No. 09/126,888, filed 7/31/1998, presently abandoned, for which a continuation Ser. No. 09/464,794 was filed on 12/16/1999, which issued as U.S. Pat. No. 6,424,717; and

Ser. No. 09/126,795, filed 7/31/1998, which issued as U.S. Pat. No. 6,105,134.

FIELD OF THE INVENTION

The present invention relates generally to the field of encrypted streams in a communications system, and more specifically towards methods and apparatus for transmitting dual encrypted streams in a communications system.

BACKGROUND OF THE INVENTION

The control of the content is important in order to protect the programming from, for example, nonpaying customers. A conventional communications system, such as a cable television system, therefore, typically applies an encryption scheme to television content in order to prevent unrestricted access. Once a system operator chooses an encryption scheme, the operator installs all of the necessary headend equipment (e.g., Scientific-Atlanta's conditional access software and equipment). The devices (set-tops) located at the subscriber's premises must be compatible with the encryption scheme in order to decrypt the content for viewing. Due to the proprietary systems, however, an operator is prevented from installing different set-tops that do not have the proper decryption scheme. If the operator wishes to install different set-tops that decrypt a different conditional access system, the operator would also have to install a second proprietary system to overlay the incumbent system in order to use both boxes.

It would be to the operator's advantage to be able to choose boxes from any manufacturer and easily implement different encryption schemes in the system without duplicating the headend equipment and utilizing extra bandwidth. Some have attempted to address a technique that overlays two encryption schemes in a system. The present application is directed towards

improvements to and alternative embodiments of a conditional access system that enables different proprietary set-tops that decrypt content that has been encrypted by different encryption schemes.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a prior art dual encryption process.

FIG. 2 is an illustration of a program including a critical packet.

FIG. 3 is an illustration of the critical packet and the duplicated packet of FIG. 2. .

FIG. 4 is a block diagram of a first embodiment of a dual encryption scheme in accordance with the present invention.

FIG. 5 is an illustration of one program aligner, identifier, and remapper (AIR) device in accordance with the present invention that is suitable for use in an AIR device of FIG. 4.

FIG. 6 is an illustration of a second embodiment of a dual encryption scheme in accordance with the present invention.

FIG. 7 is an illustration of one program aligner, identifier, and remapper (AIR) device in accordance with the present invention that is suitable for use in the AIR device of FIG. 6.

FIG. 8 provides an example table illustrating the single programs that may be provided to an output port of demultiplexers.

FIG. 9 is a state diagram illustrating the comparing of the packets by the packet comparator of FIG. 5.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

The present invention will be described more fully hereinafter with reference to the accompanying drawings in which like numerals represent like elements throughout the several figures, and in which an exemplary embodiment of the invention is shown. This invention may, however, be embodied in many different forms and should not be construed as being limited to the embodiments set forth herein; rather, the embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. The present invention is described more fully hereinbelow.

The present invention is directed towards a partial dual encryption scheme. Methods and apparatus are described that provide a transport stream including a clear stream and dually-

encrypted streams. The present invention allows for two different set-tops (i.e., an incumbent set-top and an overlay set-top) to be located in a single system. Each set-top is designed to decrypt a proprietary encryption scheme. Advantageously, the present invention is accomplished without duplicating all of the headend equipment, and without consuming twice the original bandwidth. It will be appreciated that the incumbent set-tops remain unchanged and are simply conventional devices that are most likely already deployed in the system.

A clear multiprogram transport stream (MPTS) is provided to a headend facility. It will be appreciated that the clear MPTS includes several streams of unencrypted programs each including video, audio, and data packets. The packets each have a packet identifier (PID). Typically, an encryption scheme encrypts some or all of the packets (herein referred to as critical packets) of some or all of the programs depending upon the level of desired security. Further information regarding a conditional access system can be found in U.S. Pat. App. Ser. No. 10/602,986 entitled "Method for Partially Encrypting Program Data" filed 6/25/03 and U.S. Pat. No. 6,424,717 entitled "Conditional Access System" filed 12/16/1999, which are commonly assigned, the disclosure and teachings of which are hereby incorporated by reference.

FIG. 1 is directed towards a dual encryption scheme, and is taught in U.S. Pat. Application Publication No. US 2003/0026423 A1 by Unger. A clear stream 105 is provided to a critical packet identifier, duplicator, and remapper device (IDR) 110. The identifier device 100 identifies a critical packet in a program. FIG. 2 is an illustration of a stream including a critical packet 205 having a PID no. 210 (e.g., PID 100). The predetermined critical packet 205 is identified from the stream and duplicated. FIG. 3 is an illustration of the critical packet and the duplicated packet of FIG. 2. The IDR 110 of FIG. 1 then remaps the two critical packets (i.e., the critical packet 205 and the duplicated packet 305) to have differing PID values 310, 315. If, for example, the PID has an original value of 100, the IDR 100 may remap the critical packet 205 to have a PID value of 101 (310) and the duplicated packet 305 to have a PID value of 102 (315). It is also noted that the duplicated packet 305 is placed immediately following the critical packet 205 as taught by Unger.

Referring again to FIG. 1, Scrambler A 115 is then programmed to detect the PID values of the critical packets (e.g., PID 101) and scramble them with a first encryption scheme. Scrambler B 120 then detects the duplicated packets having the remapped PID value (e.g., PID 102) and scrambles them according to a second encryption scheme. The transport stream including the clear stream (C) and the two encryption streams (A and B) are subsequently provided to a PID remapper 125. The PID remapper 125 remaps the clear stream (C) to have the same PID value as the first encryption stream A (e.g., PID 100 to PID 101). The transported stream may then include, for example, a percentage, such as 98%, of the clear stream C and a percentage, such as 2%, of both of the encrypted streams A and B. In this manner, an incumbent set-top, which is designed to decrypt encryption scheme A, receives 98% of the clear stream and 2% of the encrypted stream A. The remaining 2% of the encrypted stream B is simply not processed and discarded.

There are, however, several disadvantages with the teachings of Unger. More specifically, Unger relies on controlling the incumbent headend encryption equipment to the level of specifying exactly which PIDs to encrypt, which would be extremely difficult to accomplish in some existing encryption systems. For example, a Scientific-Atlanta encryption system, as described in U.S. Pat. No. 6,424,717, does not provide a control interface to encrypt a specific PID. The encryption schemes are performed at the program level and would require extensive recreations of a program mapping table and its associated sessions. In contrast, the present invention does not require any changes to the incumbent headend equipment or require any special control. More specifically, the present invention simply utilizes the output of the existing headend equipment without modifications. Another disadvantage, is that the teachings of Unger require two operations on the clear stream by the overlayed headend equipment; specifically, a first time for the critical packet selection and again for the PID remapping. The present invention, however, only processes the streams once using one piece of equipment. Advantageously, this is an improvement that reduces the cost and the complexity of the system.

A further advantage of the present invention is that modification of the encryption percentage is accomplished as a function of available bandwidth in the system. For example, if there is additional bandwidth available, the present invention can increase the encrypted percentage from, for example, 2% to 6%. Notably, this feature is important to the system operators who need to be sensitive of both the required bandwidth and the security level of the programs.

Referring now to FIG. 4, a block diagram is illustrated depicting a first embodiment of a partial dual encryption scheme in accordance with the present invention. An MPTS, which is a clear stream C that includes a plurality of programs, is provided to scrambler A 410 and scrambler B 415. Scrambler A 410 and scrambler B 415 encrypts the clear stream C and respectively provides encrypted stream A and encrypted stream B. In a typical application, scrambler A 410 is the existing scrambler of the incumbent encryption scheme, and scrambler B is the additional scrambler required for the additional encryption scheme. A demultiplexer 420 is coupled to scrambler A 410 to demultiplex the encrypted stream A, which as mentioned includes a combination of programs, to provide a single program to a single output port. Similarly, demultiplexers 425 and 430 demultiplex the programs to provide the same single programs to an output port.

FIG. 8 provides an example table illustrating the single programs that may be provided to an output port of the demultiplexers 420, 425, 430 for further processing. For example, a first Program P1 805, which may include video PID 100, audio PID 110, and other PID 120, (which may be a data PID or second audio PID), may be sent to a first output port of demultiplexers 420, 425, 430. Similarly, a second Program P2 810, which may include video PID 200, audio PID 210, and other PID 220, may be sent to a second output port of demultiplexers 420, 425, 430. It will be appreciated that there can be any number of programs that can be provided to an output port.

Referring again to FIG. 4, an aligner, identifier, and remapper (AIR) device 435 receives the programs from the output ports of the demultiplexers 420, 425, 430, where the programs, or

streams, (P1, P2, Pn) are grouped at the input of the AIR device 435, and is discussed below. The output streams of the AIR device 435 are provided to a multiplexer 440 that then provides a multiplexed partial dual encrypted transport stream. Additionally, the demultiplexer 420 coupled to scrambler A, which in this embodiment is assumed to be the incumbent scrambling scheme, also includes an output port 442 that provides undefined packets directly to the multiplexer 440. Due to the fact that there may be packets that are intended for purposes that are specific to the incumbent set-tops, these packets should be allowed to continue through the system without any potential alterations or deletion.

FIG. 5 is an illustration of one program aligner, identifier, and remapper (AIR) device 500 in accordance with the present invention that is suitable for use in the AIR device 435 of FIG. 4. It will be appreciated that the present invention in comparison with the prior art does not duplicate or remap critical packets. Additionally, it will be appreciated that more than one program AIR device 500 can be implemented in the AIR device 435 depending upon the number of programs (e.g., P1, P2, Pn) to be processed. Buffer A 505, buffer B 510, and buffer C 515 receive the streams A, B, and C from the output the demultiplexers 420, 425, 430. The buffers 505, 510, 515 allow a packet comparator 520 to monitor the streams A, B, and C and align them in time. Alignment may be necessary since the encrypted streams A and B may be somewhat delayed and out of synchronization due to the scramblers 410, 415.

FIG. 9 is a state diagram illustrating the comparing and aligning of the packets by the packet comparator 520. In the initial state 905, the buffers 505, 510, 515 are filled with packets, and the packet comparator 520 begins searching, in state 910, for a reference packet (ref pkt) in the clear stream, which is provided by buffer C 515. The reference packet may be, for example, a video PID with a payload_unit_start_indicator (PUSI) bit equal to one (1). It will be appreciated that the specifications for this reference packet may have other specifications, such as an audio PID and the PUSI bit may be equal to 0. The basis for comparison however must be valid for packets in the clear or scrambled state. Further information regarding the PUSI bit can be found in U.S. Pat. No. 6,424,714 entitled "Conditional Access System." If the reference packet is not

found, the clear stream C passes, and the encrypted streams A and B drop in state 915. The searching state 910 continues until the reference packet is found in the clear stream C. Subsequently, in state 920, the encrypted streams A and B are compared to the found reference packet. The basis for comparison is again the video PID, and the presence of the PUSI bit equal to one (1). The basis for comparison is not affected by the fact that scrambler A 410 or B 415 has scrambled the packet. If the packets in either of the streams A and B do not match, the non-matching packet(s) drop in state 925. If buffers A 505 and B 510 are empty, the state returns to state 910 and begins searching. Otherwise, state 920 continues comparing the packets in streams A and B with the reference packet until a match is found, and the streams are then considered aligned.

In the aligned state 928, state 930 waits until buffers A 505, B 510, and C 515 have greater than one packet. Subsequently, the head packets are verified to have the same PID value, in state 935. If not, in state 940, the packet in stream C passes and packets in streams A and B drop, and state 935 continues verifying the packets. At times, packets in a program can be swapped in their position and are essentially out of order. In that case , passing the packets in the clear stream C ensure that the packets are passed rather than stalling in the buffers. If the head packet PID values are the same, the values of the continuity_counter field of the packets are then verified to be the same, in state 945. If not, the assumption is that there is an error in the alignment, and the comparator 520 returns to the initial state 905. It will be appreciated that the continuity counter of the clear stream C is used as the reference number. If the continuity counters are the same for the all the packets in the streams, state 950 releases the packets from the buffers A, B, and C, and returns to the aligned state 930 to continue ensuring alignment of the packets. It will be appreciated that there are other methods for verifying alignment, other than the use of the continuity_count value, such as the presence and length of an adaptation_field, or the presence and value of a program_clock_reference (PCR) value.

It should be noted that MPEG packet processing equipment typically modifies the Program Clock Reference (PCR) of programs being processed, to correct for any PCR jitter that

would otherwise be introduced. In this embodiment, the PCRs of clear stream C are regarded as the primary PCRs, and all PCR modifications are performed on the values in stream C. If the PCR-bearing packet is also a critical packet, the corrected PCR value from stream C is placed into the PCR field in the packet from streams A and B.

Referring again to FIG. 5, a remapper 525 remaps the PID value of the released packet from stream B to a new PID value, for example, PID 100 to PID 101 and/or PID 110 to PID 111, depending upon whether the critical packet selection includes just video or audio packets or includes both video and audio packets. A switch 535, 540, 545 then gates the released packets of stream A, B, and C.

A selector 530 also receives the released packet of clear stream C, which it uses as a reference stream to control the switches 535, 540, 545. In the preferred embodiment of the present invention, the selector 530 allows the packets of the clear stream C to pass through to a multiplexer 550 until such time as a critical packet is detected. Again, it will be appreciated that the critical packet can be a video, audio, and/or data packet. When the critical packet is detected, the switch 545 opens and switches 535, 540 are closed, thereby allowing the released packets of encrypted streams A and B, which each have the aligned critical packet, to simultaneously pass through to the multiplexer 550. The multiplexer 550 then combines the packets to provide a partial dual-encrypted transport stream where the dual encryption includes packets encrypted by both scrambler A 410 and scrambler B 415. The multiplexed stream is then provided to multiplexer 440 (FIG. 4) to be combined with additional partial dual-encrypted program streams. It will be appreciated that multiplexer 550 provides only a portion of the packet stream to the overall multiplexer 440 of FIG. 4. In this manner, when bandwidth becomes available in multiplexer 440, a signal indicating an increase in encrypted packets is allowable is provided to multiplexer 550 via feedback loop 560. The multiplexer 550 then relays this information to the selector 530 via feedback loop 565, and the selector 530 can then increase the percentage of critical packets, for example, from 2% to 6% of the packets that are considered critical.

FIG. 6 is an illustration of a second embodiment of a partial dual encryption scheme in accordance with the present invention. The advantage of the configuration shown in FIG. 6 is that all the elements required to add an additional encryption scheme (Demux 607, 608, AIR devices 615, and Mux 640) can be implemented in a single piece of equipment. An MPTS C is provided to scrambler A 605 that provides a first encrypted stream A. A first demultiplexer 607 receives the encrypted stream A and a second demultiplexer 608 receives the clear stream C in order to demultiplex the plurality of programs into single programs. Again, assuming the scrambler A 605 is the incumbent encryption scheme, an output port 609 of the demultiplexer 607 is provided for unidentified packets and is provided directly to a multiplexer 640 for delivery along with the partial dual-encrypted transport stream. The common programs from the demultiplexers 607, 608 are then provided to an aligner, identifier, and remapper (AIR) device 615.

FIG. 7 is an illustration of one program aligner, identifier, and remapper (AIR) device 700 in accordance with the present invention that is suitable for use in the AIR device 615 of FIG. 6. For a first program P1, the encrypted stream A is buffered in buffer A 710, and buffer C 715 receives the clear stream C. A packet comparator 720 compares the packets to ensure they are aligned due to any delays introduced by scrambler A 705. It will be appreciated that the packet comparator 720 operates in a similar manner to the packet comparator 520 of FIG. 5 and in accordance with the state diagram of FIG. 9 for just encrypted stream A. A critical packet selector 725 uses the clear stream C as a reference stream and controls two switches 730, 735 accordingly. More specifically, switch 730 allows the packets of clear stream C to pass through to a multiplexer 740 until a critical packet is detected. When the critical packet is detected, switch 730 provides the packet of clear stream C to scrambler B 745 and switch 735 is also switched, thereby allowing the critical packet of encrypted stream A to pass through to the multiplexer 740. The scrambler B 745 encrypts the packet of clear stream C according to a second encryption method and provides the encrypted packet to a PID remapper 750. The PID remapper 750 remaps the packet's PID value to a new PID value (e.g., PID 100 to PID 101 and/or PID 110 to 111). The remapped packet is subsequently provided to the multiplexer 740 for transmitting along with the

packet of the encrypted stream A. The scrambler B 745 also controls the PID comparator 720 in order to prevent packets from being transmitted until the scrambler B 745 and the remapper 750 have completed their steps, thereby maintaining proper ordering of packets.

A partial dual-encrypted transport stream is then provided to the multiplexer 640 (FIG. 6) to be combined with other partial dual-encrypted programs. The combined partial dual-encrypted transport stream is then provided to the set-tops and decrypted according to the decryption methods (i.e., encryption method A or encryption method B) of the set-top. Similar to the first embodiment of the present invention, multiplexer 740 provides only a portion of the packet stream to the overall multiplexer 640 of FIG. 6. In this manner, when bandwidth becomes available in multiplexer 640, a signal indicating an increase in encrypted packets is allowable is provided to multiplexer 740 via feedback loop 650. The multiplexer 740 then relays this information to the remapper 750 via feedback look 765, and the remapper 750 can then increase the percentage of critical packets, for example, from 2% to 6% of the packets that are considered critical.

It will be appreciated that modifications can be made to the two embodiments that are still within the scope of the invention. Additionally, the present invention can be implemented using hardware and/or software that are within the scope of one skilled in the art. The embodiments of the description have been presented for clarification purposes; however, the invention is defined by the following claims.

What is claimed is: